Japanese Patent Application, Laid-Open Publication No. H11-266483

INT. CL.[6]: H04Q 7/38
G06F 13/00
H04L 9/08

PUBLICATION DATE: September 28, 1999

TITLE	Information Distribution Method and Portable Terminal Device
APPLICATION NO.	H10-68231
FILING DATE	March 18, 1998
APPLICANT(S)	TOSHIBA CORP.
INVENTOR(S)	Takefumi SAKAMOTO and Mutsumi SERIZAWA

ABSTRACT

PROBLEM To achieve billing of users at low cost when newly constructing a mobile communication system capable of high-speed communication in addition to existing mobile communication systems.

SOLUTION Information requested by a user is sent to a portable terminal via a radio base station capable of high-speed communication in an encrypted format, and a key for decrypting the information is sent to the portable terminal via a radio base station of an existing mobile communication system.

CLAIMS

1. An information distribution method for distributing information to a portable terminal device comprising first communication means for transmitting and/or receiving signals in a first communication format, and second communication means for transmitting and/or receiving signals in a second communication format different from said first communication format;

the information distribution method being characterized in that encrypted information which has been encrypted with respect to said portable terminal device is transmitted via said first communication means, and key information for decoding said encrypted information is transmitted to said portable terminal via said second communication means.

2. An information distribution method for distributing information to a portable terminal device comprising first communication means for transmitting and/or receiving signals in a first communication format, and second communication means for transmitting and/or receiving signals in a second communication format different from said first communication format;

the information distribution method being characterized in that encrypted information which has been encrypted with respect to said portable terminal device is transmitted via said first communication means, verification of said portable terminal device is performed via said second communication means and key information for decoding said encrypted information is transmitted to said portable terminal via said second communication means based on said verification results.

3. An information distribution method as recited in claim 1 or 2, characterized in that said first communication format is a faster communication format than said second communication format.

4. An information distribution method as recited in any one of claims 1-3, characterized in that when transmitting key information for decoding said encrypted information to said portable terminal device via said second communication means, said portable terminal device is billed.

5. An information distribution method as recited in any one of claims 1-4, characterized in that if the encrypted information received by said information terminal device via said first communication means is not safely decoded using the key information received via said second communication means,

said portable terminal device transmits a request for retransmission of said key information through said second communication means.

6. An information distribution method as recited in any one of claims 1-5, characterized in that if the encrypted information received by said information terminal device via said first communication device is safely decoded using key information receiving via said second communication means, said portable terminal device transmits a decoding complete notification through said second communication means.

7. An information distribution method as recited in claim 6, characterized in that if a decoding completion notification is not received from said portable terminal device within a predetermined time after transmission of key information from a key management server for managing said key information to said portable terminal, said key management server retransmits the key information through the second communication means.

8. A portable terminal device characterized by comprising:

first communication means for transmitting and receiving signals in a first communication format; and

second communication means for transmitting and receiving signals in a second communication format different from said first communication format;

wherein encrypted information which has been encrypted is transmitted and/or receiving via said first communication means, and key information for decoding said encrypted information is transmitted and/or received via said second communication means.

9. A portable terminal device as recited in claim 8, characterized in that said first communication

format is a faster communication format than said second communication format.

10. A portable terminal device as recited in claim 9 and 10, characterized by further comprising retransmission request means for requesting retransmission of said key information via said second communication means if the encrypted information received via said first communication means is not safely decoded using key information received through said second communication means.

11. A portable terminal device as recited in claim 9 and 10, characterized by further comprising decoding completion notification means for issuing a decoding completion notification through said second communication means if the encrypted information received through said first communication means is safely decoded using the key information received via said second communication means.

DETAILED DESCRIPTION OF THE INVENTION

Technical Field

The present invention relates to an information distribution method in a communication system for transmitting information such as data, audio and images to a portable information terminal, and relates to an information distribution method in an information providing system, particularly using radio or light.

Conventional Art

In recent years, information terminals such as personal computers and electronic notebooks have been becoming smaller, and it has become easier for terminal users to use these information terminals in mobile environments. With these developments, the demand for systems offering large capacities of information immediately to these portable information terminals will also increase. Therefore, mobile communication systems capable of high-speed information transmission will be put into practice.

Fig. 16 is a structural diagram showing the structure of a mobile communication system having a mobile communication system capable of high-speed information transmission newly added to a conventional

mobile communication system. The information providing system according to this conventional example comprises a second verification server 201, a first verification server 207, at least one information server 202, a communication network 205, a first radio vase station 203, a second radio vase station 204 and at least one portable terminal 206. The information server 202 stores information provided to a plurality of portable terminals 206 via a first radio base station 203 or a second radio base station 204. The information terminal 206 is capable of communicating with a first radio base station 203 and a second radio base station 204. Additionally, the second verification server 201 performs verification of the portable terminal 206 which communicates via the second radio base station 204.

Here, the existing mobile communication system comprises a second verification server 201 and a plurality of second radio base stations 204. Here, if a first radio base station 204 capable of faster communication than the second radio base station is newly added, a first verification server 207 for performing verification of the portable terminal 206 for communicating via said first radio base station 203 must be added.

As described above, when constructing a mobile communication system capable of high-speed communications, a verification server must be newly constructed in order to perform appropriate billing.

Problems to be Solved by the Invention

The present invention has the object of resolving problems such as indicated above, by efficiently billing users in a mobile communication system offering large quantities of information immediately to users by using an existing mobile communication system and a high-speed radio or light link in conjunction.

Means for Solving the Problems

In order to achieve the above-described object, the present invention offers an information distribution method for distributing information to a portable terminal device comprising first communication means for transmitting and/or receiving signals in a first communication format, and second communication means for transmitting and/or receiving signals in a second communication format different from said first communication format; the information distribution method being characterized in that encrypted information which has been encrypted with respect to said portable terminal device is transmitted via said first communication means, and key information for decoding said encrypted information is transmitted to said portable terminal via said second communication means.

Furthermore, the present invention offers an information distribution method for distributing information to a portable terminal device comprising first communication means for transmitting and/or receiving signals in a first communication format, and second communication means for transmitting and/or receiving signals in a second communication format different from said first communication format; the information distribution method being characterized in that encrypted information which has been encrypted with respect to said portable terminal device is transmitted via said first communication means, verification of said portable terminal device is performed via said second communication means and key information for decoding said encrypted information is transmitted to said portable terminal via said second communication means based on said verification results.

Furthermore, the present invention is characterized in that said first communication format is a faster communication format than said second communication format. Furthermore, the present invention is characterized in that when transmitting key information for decoding said encrypted information to said portable terminal device via said second communication means, said portable terminal device is billed.

Furthermore, the present invention is characterized in that if the encrypted information received by said information terminal device via said first communication means is not safely decoded using the key information received via said second communication means, said portable terminal device transmits a request for retransmission of said key information through said second communication means.

Furthermore, the present invention is characterized in that if the encrypted information received by said information terminal device via said first communication device is safely decoded using key information receiving via said second communication means, said portable terminal device transmits a decoding complete notification through said second communication means.

A portable terminal device of the present invention is characterized in that if a decoding completion notification is not received from said portable terminal device within a predetermined time after transmission of key information from a key management server for managing said key information to said portable terminal, said key management server retransmits the key information through the second communication means.

Furthermore, the present invention is characterized by comprising first communication means for transmitting and receiving signals in a first communication format; and second communication means for transmitting and receiving signals in a second communication format different from said first communication format; wherein encrypted information which has been encrypted is transmitted and/or

receiving via said first communication means, and key information for decoding said encrypted information is transmitted and/or received via said second communication means.

Furthermore, the portable terminal device of the present invention is characterized in that said first communication format is a faster communication format than said second communication format.

Furthermore, the portable terminal device of the present invention is characterized by further comprising retransmission request means for requesting retransmission of said key information via said second communication means if the encrypted information received via said first communication means is not safely decoded using key information received through said second communication means.

Furthermore, the portable terminal device of the present invention is characterized by further comprising decoding completion notification means for issuing a decoding completion notification through said second communication means if the encrypted information received through said first communication means is safely decoded using the key information received via said second communication means.

Embodiments of the Invention

Herebelow, an embodiment of the present invention shall be explained with reference to the drawings. Fig. 1 is a structural diagram showing the structure of an information providing system according to an embodiment of the present invention. The information providing system according to the present embodiment comprises a key management server 101, an information server 102, a communication network 105, a first radio base station 103, a second radio base station 104, and at least one portable terminal 106. The portable terminal 106 is capable of communicating with the first radio base station 103 and the second radio base station 104, and the first radio base station 103 is capable of transmitting information faster than the second radio base station 104. On the other hand, the second radio base station 104 offers communication services over a wider geographical range than the first radio base station 103. The information server 102 stores information to be provided to the portable terminal 106 in encrypted form, and the key management server 101 stores keys for decoding this encrypted information. The key management server 101, information server 102, first radio base station 102 and second radio base station 104 are connected via the communication network 105.

Next, an example of the operation of the information distribution method in the information providing system of the above arrangement shall be described. Fig. 2 and Fig. 3 are flow diagrams showing an information distribution method according to an example of an embodiment of the present invention.

When a user requests information, the portable terminal 106 owned by the user transmits an information request to the second radio base station 104, and the second base station further transmits the information request to the information server 102. Here, the portable terminal 106 may also transmit the information request to the first radio base station 103 as shown in Fig. 4. The information server 102 transmits the requested information through the first radio base station 103 to the portable terminal 106 in encrypted form. Since the portable terminal 106, upon receiving the encrypted information which has been encrypted, requires a key for decoding the encrypted information, it sends a key request to the second radio base station 104. The second radio base station 104 which has received the key request further sends the key request to the key management server 101. The key management server 101 sends the requested key through the second radio base station 104 to the portable terminal 106. Here, as in the example of the information distribution method shown in the flow diagram of Fig. 4 or Fig. 5, the key management server 101 may perform a verification as to whether or not the portable terminal 106 is a valid terminal via the second radio base station 104. If the key management server 101 finds the portable terminal 106 to be a valid terminal, it sends the requested key through the second radio base station 104 to the portable terminal 106. Upon receiving the key, the portable terminal 106 is capable of decoding the received information which is encrypted. IN the key management server 101, it is also possible to perform billing after the key has been sent to the portable terminal.

Additionally, as shown in the flow diagram of Fig. 6, when the portable terminal 106 receives the key and performs decoding, and the decoding is normally completed, it sends a decoding completion notification through the second radio base station 104 to the key management server 101, and the key management server 101 may perform billing after having received the decoding completion notification.

On the other hand, in the case of an information providing system wherein the portable terminal 106 makes a contract beforehand, it is possible to have the key management server find whether or not the portable terminal 106 has a contract upon receiving the key request, and to send the key to the portable terminal 106 only if a contract has been made. In the above, an example wherein the key is received after the portable terminal 106 has received information is described, but the portable terminal 106 may receive the information after receiving the key. Additionally, it is possible to have the portable terminal 106 request and receive a plurality of encrypted information, then to request and receive the key for decoding only the information which is to be viewed when the user wants to view information, and to decode only the encrypted information which is to be viewed.

As described above, due to the portable terminal receiving encrypted information from a radio base station capable of high-speed communication, and receiving a key for decoding information from a radio base

station capable of offering the communication service over a geographically wide range, reception of information in a short time and decoding of the encrypted information over a wide geographical range is possible, and it is possible to transmit information only to valid users. Additionally, the key and billing management can be performed in only a communication system offering communication services over a wide geographic range. In particular, when an existing PHS (Personal Handyphone System) base station or car/cellular telephone base station is used as the second radio base station 104, it is possible to use an existing communication system for billing by using existing user information and adding a first radio base station capable of high-speed communications, thus making it possible to construct a high-speed information providing system at a low cost.

Next, an example of the operations of an information distribution method wherein key requests are not issued from the portable terminal is shown. Fig. 7 and Fig. 8 are flow diagrams showing an information distribution method according to another embodiment of the present invention.

The structure of the information providing system according to the present embodiment is identical to that of the structural diagram in Fig. 1.

When a user requests information, the portable terminal 106 owned by the user transmits an information request to the second radio base station 104, and the second base station further sends the information request to the information server 102. Here, the portable terminal 106 may send the information request to the first radio base station 103 as shown in Fig. 7. While the information server 102 sends the requested information through the first radio base station 103 to the portable terminal 106 in encrypted form, it also sends a key request to the key management server to request that a key for decoding the encrypted information be sent to the portable terminal 106. This is possible by the portable terminal 106 giving an identifier for communicating via the second radio base station when issuing the information request. The key management server 101, upon receiving the key request, sends the requested key through the second radio base station 104 to the portable terminal 106.

Here, as in the example of the information distribution method shown in the flow diagram of Fig. 9 or Fig. 10, the key management server 101 may perform a verification as to whether or not the portable terminal 106 is a valid terminal, through the second radio base station 104. If the key management server 101 finds the portable terminal 106 to be a valid terminal, it sends the requested key through the second radio base station 104 to the portable terminal 106. When the portable terminal 106 receives this key, it can decode the received information which has been encrypted. Here, the key management server 101 may perform billing after transmitting the key to the portable terminal 106. Additionally, as shown in the flow

diagram of Fig. 6, it is possible to have an arrangement such that when the portable terminal 106 has received the key and performed decoding, and the decoding has been completed normally, it transmits a decoding completion notification through the second radio base station 104 to the key management server 101, and the key management server 101 performs billing after having received the decoding completion notification. On the other hand, in the case of an information providing system in which the portable terminal 106 has been contracted beforehand, it is possible to have an arrangement wherein the key management server finds whether or not the portable terminal 106 has been contracted upon receiving a key request, and sends the key to the portable terminal 106 only when there is a contract.

As described above, due to the portable terminal receiving encrypted information from a radio base station capable of high-speed information, and receiving a key for decoding the information from a radio base station capable of providing communication services over a wide geographic range, it is possible to receive information in a short time and to decode the encrypted information over a wide geographic range, as well as to transmit the information only to valid users. Additionally, the key or billing management should be performed in only the communication system providing communication services over a wide geographic range. In particular, when an existing PHS (Personal Handyphone System) base station or car/cellular telephone base station is used as the second radio base station 104, it is possible to use an existing communication system for billing by using existing user information and adding a first radio base station capable of high-speed communications, thus making it possible to construct a high-speed information providing system at a low cost. Furthermore, it is possible to construct an information providing system where there is no need to request a key by calling from the portable terminal, thus making it easier for users to use.

Next, an example of the actions for an information distribution method when the portable terminal which has received the encrypted information and key cannot decode the information shall be indicated. Fig. 11 is a flow diagram showing an information distribution method according to another embodiment of the present invention. The structure of the information providing system according to the present embodiment is the same as in the structural diagram shown in Fig. 1.

The key management server 101, upon transmitting the key through the second radio base station 104 to the portable terminal 106, bills the portable terminal 106 or the user of the portable terminal 106. The portable terminal 106 which has received the key decodes the information using the key. Here, if the information cannot be decoded normally, the portable terminal 106 sends a decoding impossible notification through the second base station 104 to the key management server 101, to transmit that the information cannot be decoded. If the key management server 101 has performed billing after

transmission of the key, it cancels the billing.

As described above, when the portable terminal is not able to decode the information with the received key, it can cancel billing even if the billing has already occurred by means of transmitting a decoding addition notification through the second radio base station. Additionally, since the second radio base station covers a wider geographical range than the first radio base station, there is a greater probability that a notification an be made in the event that decoding is not possible, thus enabling invalid billing to be prevented.

Next, another operation of the information distribution method for the case where the portable terminal which has received the encrypted information and key cannot decode the information shall be described. Fig. 12 is a flow diagram showing an information distribution method according to another embodiment of the present invention. The structure of the information providing system according to the present embodiment is the same as in the structural diagram of Fig. 1.

The key management server 101 transmits a key through the second radio base station 104 to the portable terminal 106. Here, the key management server 101 may perform billing of the portable terminal 106 or the user of the portable terminal 106. The portable terminal 106 which has received this key uses the key to decode the information. Here, if the information cannot be normally decoded, the portable terminal 106 transmits a key retransmission request through the second radio base station 104 to the key management server 101, and requests a key to decode the encrypted information. Based on this request, the key management server 101 transmits the key through the second radio base station 104 to the portable terminal 106. Here, as in the example of the information distribution method shown in the flow diagram of Fig. 13, the key management server 101 may perform a verification as to whether or not the portable terminal 106 is a valid terminal via the second radio base station 104. If the portable terminal 106 is found to be a valid terminal, the key management server 101 retransmits the requested key through the second radio base station 104 to the portable terminal 106. The portable terminal 106 which has received the retransmitted key decodes the information using the key. Here, if the decoding fails once again, the portable terminal 106 may again send the key management server a retransmission request.

Alternatively, it may send the key management server 101 a decoding impossible notification, and if already billed, may also request cancellation of the bill. As described above, if the portable terminal is not able to decode the information with the received key, it can obtain the key once again by sending a key retransmission request through the second radio base station. Additionally, since the second radio base station covers a wider geographic range than the first radio base station, there is a high probability of being

able to receive the key once again in the case where decoding fails, thus increasing the possibility that the information can be correctly decoded by the portable terminal.

Next, another example of the actions of the information distribution method for the case where the portable terminal which has received encrypted information and a key cannot decode the information shall be described. Fig. 14 is a flow diagram showing an information distribution method according to another embodiment of the present invention. The structure of the information providing system according to the present embodiment is the same as in the structural diagram shown in Fig. 1.

The key management server 101 sends a key through the second radio base station 104 to the portable terminal 106. The portable terminal 106 which has received this key uses this key to decode the information. Here, as shown in the flow diagram of Fig. 6, when the information is safely decoded in the portable terminal 106, the portable terminal 106 sends a decoding completion notification through the second radio base station 104 to the key management server 101, and the key management server 101 may perform billing upon receiving the decoding completion notification within a predetermined period of time. However, if the information cannot be normally decoded in the key portable terminal 106, the decoding completion notification is not sent. For this reason, the key management server 101 times out upon the passage of a predetermined period of time after transmitting the key, and retransmits the key. Here, as in the example of the information distribution method shown in the flow diagram of Fig. 15, the key management server 101 may perform a verification as to whether or not the portable terminal 106 is a valid terminal through the second radio base station 104 before retransmitting the key. If the key management server 101 finds the portable terminal 106 to be a valid terminal, it retransmits the requested key through the second radio base station 104 to the portable terminal 106. The portable terminal 106 once again receives the key and is able to decode the received information. Here, if the information is able to be safely decoded at the portable terminal 106, the portable terminal 106 may transmit a decoding completion notification to the key management server 101 as shown in the flow diagram of Fig. 6. On the other hand, if the decoding fails, the portable terminal 106 does not send a decoding completion notification, thus enabling a key to be received once again from the key management server.

As explained above, if the portable terminal is not able to decode the information with the received key, the key can be obtained again. Additionally, since the second radio base station covers a wider geographical range than the first radio base station, the probability of being able to receive the key once again when the decoding fails is high, and the possibility of correctly decoding the information at the portable terminal can be increased.

Effects of the Invention

As described above, with the information distribution method of the present invention, a large quantity of information requested by the user can be transmitted to the portable terminal in an extremely short time, while accurately performing billing. Additionally, it is possible to make use of existing low-speed communication systems while performing billing management at low cost.

Furthermore, since the verification can be performed separately from transmission of information to the portable terminal, the time required to transmit information to the portable terminal can be shortened, thus making it possible to improve the efficiency of use of channels for transmitting information.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 An explanatory diagram showing the structure of an information providing system according to an embodiment of the present invention.

Fig. 2 A flow diagram showing an information distribution method according to an embodiment of the present invention, particularly a flow diagram for the case where the portable terminal makes an information request through a second radio base station.

Fig. 3 A flow diagram showing an information distribution method according to an embodiment of the present invention, particularly a flow diagram for the case where the portable terminal makes an information request through a first radio base station.

Fig. 4 A flow diagram showing an information distribution method according to an embodiment of the present invention, particularly a flow diagram for the case where the key management server performs verification of the portable terminal.

Fig. 5 A flow diagram showing an information distribution method according to an embodiment of the present invention, particularly a flow diagram for the case where the key management server performs verification of the portable terminal.

Fig. 6 A flow diagram showing an information distribution method according to an embodiment of the

present invention, particularly a flow diagram for the case where the portable terminal sends a decoding completion notification.

Fig. 7 A flow diagram showing an information distribution method according to an embodiment of the present invention, particularly a flow diagram for the case where the portable terminal makes an information request through the second radio base station.

Fig. 8 A flow diagram showing an information distribution method according to an embodiment of the present invention, particularly a flow diagram for the case where the portable terminal makes an information request through the first radio base station.

Fig. 9 A flow diagram showing an information distribution method according to an embodiment of the present invention, particularly a flow diagram for the case where the key management server performs verification of the portable terminal.

Fig. 10 A flow diagram showing an information distribution method according to an embodiment of the present invention, particularly a flow diagram for the case where the key management server performs verification of the portable terminal.

Fig. 11 A flow diagram showing an information distribution method according to an embodiment of the present invention, particularly a flow diagram for the case where the portable terminal transmits a decoding impossible notification.

Fig. 12 A flow diagram showing an information distribution method according to an embodiment of the present invention, particularly a flow diagram for the case where the portable terminal makes a key retransmission request.

Fig. 13 A flow diagram showing an information distribution method according to an embodiment of the present invention, particularly a flow diagram for the case where the key management server performs verification of the portable terminal when retransmitting the key.

Fig. 14 A flow diagram showing an information distribution method according to an embodiment of the present invention, particularly a flow diagram for the case where the key management server retransmits the key due to a time out.

Fig. 15 A flow diagram showing an information distribution method according to an embodiment of the present invention, particularly a flow diagram for the case where the key management server performs verification of the portable terminal when retransmitting the key.

Fig. 16 A structural diagram showing the structure of an information providing system according to a conventional information distribution method.

Description of Reference Numbers

101	key management server
102	information server
103	first radio base station
104	second radio base station
105	communication network
106	portable terminal

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－266483

(43)公開日　平成11年(1999)９月28日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ
Ｇ０６Ｆ　13/00	３５１	Ｇ０６Ｆ　13/00	３５１Ｌ
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｂ

審査請求　未請求　請求項の数11　ＯＬ　（全９頁）

(21)出願番号　特願平10－68231

(22)出願日　平成10年(1998)３月18日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　坂本　岳文
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　芹澤　睦
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

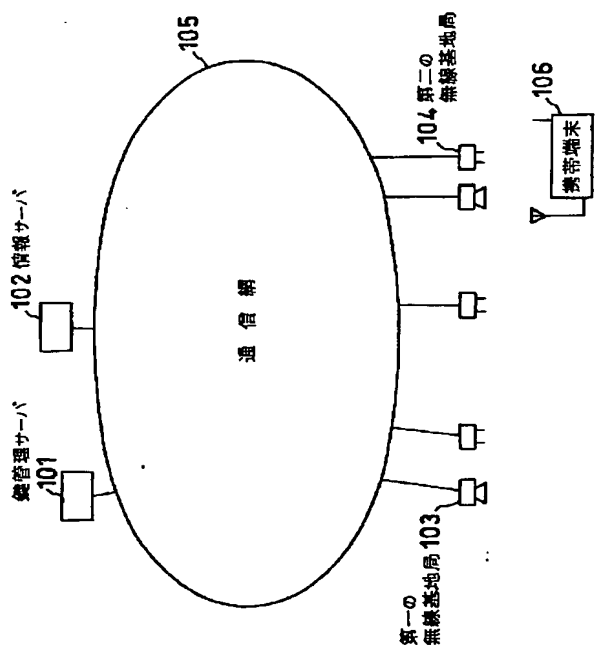
(74)代理人　弁理士　外川　英明

(54)【発明の名称】　情報配信方法及び携帯端末装置

(57)【要約】

【課題】既存の移動通信システムに加えて、高速な通信可能な移動通信システムを新たに構築する場合、利用者に対する課金を低コストで実現する。

【解決手段】利用者が要求した情報は、暗号化した形式で高速な通信可能な無線基地局を介して携帯端末に送信し、該情報を復号化するための鍵を既存の移動通信システムの無線基地局を介して携帯端末に送信する。



1

【特許請求の範囲】

【請求項１】　第一の通信方式の信号を送信及び又は受信する第一の通信手段と、前記第1 の通信方式のとは異なる第二の通信方式の信号を送信及び又は受信する第二の通信手段と備える携帯端末装置に対して情報を配信する情報配信方法において、

前記携帯端末装置に対して暗号化された暗号化情報を前記第一の通信手段を介して送信し、前記携帯端末に対して前記暗号化情報を解読するための鍵情報を前記第二の通信手段を介して送信することを特徴とする情報配信方法。

【請求項２】　第一の通信方式の信号を送信及び又は受信する第一の通信手段と、前記第1 の通信方式のとは異なる第二の通信方式の信号を送信及び又は受信する第二の通信手段と備える携帯端末装置に対して情報を配信する情報配信方法において、

前記携帯端末装置に対して暗号化された暗号化情報を前記第一の通信手段を介して送信し、前記第二の通信手段を介して前記携帯端末装置の認証を行い、前記認証結果に基づいて前記携帯端末装置に対して前記暗号化情報を解読するための鍵情報を送信することを特徴とする情報配信方法。

【請求項３】　前記第一の通信方式は前記第二の通信方式よりも高速な通信方式であることを特徴とする請求項１または２記載の情報配信方法。

【請求項４】前記携帯端末装置に対して、前記暗号化情報を解読するための鍵情報を前記第二の通信手段を介して送信した際に、前記携帯端末装置に対して課金することを特徴とする請求項１及至３記載の情報配信方法。

【請求項５】　前記情報端末装置が前記第一の通信手段を介して受信した暗号化情報が、前記第二の通信手段を介して受信した鍵情報を用いて正常に解読されなかった場合に、前記携帯端末装置は前記鍵情報の再送要求を前記第二の通信手段を介し送信することを特徴とする請求項１及至４記載の情報配信方法。

【請求項６】　前記情報端末装置が前記第一の通信手段を介して受信した暗号化情報が、前記第二の通信手段を介して受信した鍵情報を用いて正常に解読された場合に、前記携帯端末装置は解読完了通知を前記第二の通信手段を介し送信することを特徴とする請求項１及至５記載の情報配信方法。

【請求項７】　前記鍵情報を管理する鍵管理サーバが前記携帯端末への鍵情報送信の後、所定時間以内に携帯端末装置から解読完了通知を受信しない場合に、前記鍵管理サーバは鍵情報を第二の通信手段を介して再送することを特徴とする請求項６記載の情報配信方法。

【請求項８】　第一の通信方式の信号を送受信する第一の通信手段と、

前記第一の通信方式とは異なる第にの通信方式の信号を送受信する第二の通信手段とを具備し、

2

暗号化された暗号化情報を前記第一の通信手段を介して送信及び又は受信し、前記暗号化情報を解読するための鍵情報を前記第二の通信手段を介して送信及び又は受信することを特徴とする携帯端末装置。

【請求項９】　前記第一の通信方式は前記第二の通信方式よりも高速な通信方式であることを特徴とする請求項第８記載の携帯端末装置。

【請求項１０】　前記第一の通信手段を介して受信した暗号化情報が、前記第二の通信手段を介して受信した鍵情報を用いて正常に解読されなかった場合に、前記鍵情報の再送要求を前記第二の通信手段を介して行う再送要求手段を更に具備することを特徴とする請求項９及び１０記載の携帯端末装置。

【請求項１１】前記第一の通信手段を介して受信した暗号化情報が、前記第二の通信手段を介して受信した鍵情報を用いて正常に解読された場合に、解読完了通知を前記第二の通信手段を介して行う解読完了通知手段を更に具備することを特徴とする請求項９及び10記載の携帯端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は携帯型情報端末にデータ、音声、画像等の情報を送信する通信システムにおける情報配信方法に関し、特に無線あるいは光等を用いる情報提供システムにおける情報配信方法に関するものである。

【０００２】

【従来の技術】近年、パーソナルコンピュータや電子手帳等の情報端末の小型化が進み、端末利用者はこれらの情報端末を移動環境で利用しやすくなってきた。これに伴いこれらの携帯型情報端末に対して、瞬時に大容量の情報を提供するシステムに対する要求も増大しつつある。そこで、高速な情報伝送が可能な移動通信システムが実用化されつつある。

【０００３】図１６は従来の移動通信システムに、新たに高速な情報伝送が可能な移動通信システムを付加した移動通信システムの構成を示す構成図である。本従来例に係わる情報提供システムは、第二の認証サーバ２０１と、第一の認証サーバ２０７と、少なくとも一つ以上の情報サーバ２０２と、通信網２０５と、第一の無線基地局２０３と、第二の無線基地局２０４と、少なくとも１台以上の携帯端末２０６とを含んで構成される。情報サーバ２０２は第一の無線基地局２０３または第二の無線基地局２０４を介して複数の携帯端末２０６に提供する情報を蓄積する。携帯端末２０６は第一の無線基地局２０３及び第二の無線基地局２０４と通信可能である。また、第二の認証サーバ２０１は第二の無線基地局２０４を介して通信する携帯端末２０６の認証を行なう。

【０００４】ここで既存の移動通信システムは、第二の認証サーバ２０１及び複数の第二の無線基地局２０４を

含んで構成される。ここに、第二の無線基地局よりも高速な通信が可能な第一の無線基地局２０４を新たに付加する場合、該第一の無線基地局２０３を介して通信する携帯端末２０６の認証を行なう第一の認証サーバ２０７を付加する必要が生じる。

【０００５】以上のように、高速な通信可能な移動通信システムを構築する場合、適切な課金を行なうためには、新たに認証サーバを構築する必要があるという問題点があった。

【０００６】

【発明が解決しようとする課題】本発明は、以上に示すような問題点を解決し、既存の移動通信システムと無線あるいは光等の高速リンクを併用して、大容量の情報を利用者に対して瞬時に提供する移動通信システムにおいて、利用者に対する課金を効率的に行なうことを目的とする。

【０００７】

【課題を解決するための手段】上記の目的を達成するために、本発明は第一の通信方式の信号を送信及び又は受信する第一の通信手段と、前記第1 の通信方式のとは異なる第二の通信方式の信号を送信及び又は受信する第二の通信手段と備える携帯端末装置に対して情報を配信する情報配信方法において、前記携帯端末装置に対して暗号化された暗号化情報を前記第一の通信手段を介して送信し、前記携帯端末に対して前記暗号化情報を解読するための鍵情報を前記第二の通信手段を介して送信することを特徴とする。

【０００８】さらに本発明は、第一の通信方式の信号を送信及び又は受信する第一の通信手段と、前記第1 の通信方式のとは異なる第二の通信方式の信号を送信及び又は受信する第二の通信手段と備える携帯端末装置に対して情報を配信する情報配信方法において、前記携帯端末装置に対して暗号化された暗号化情報を前記第一の通信手段を介して送信し、前記第二の通信手段を介して前記携帯端末装置の認証を行い、前記認証結果に基づいて前記携帯端末装置に対して前記暗号化情報を解読するための鍵情報を送信することを特徴とする。

【０００９】さらに本発明は、前記第一の通信方式は前記第二の通信方式よりも高速な通信方式であることを特徴とする。さらに本発明は、前記携帯端末装置に対して、前記暗号化情報を解読するための鍵情報を前記第二の通信手段を介して送信した際に、前記携帯端末装置に対して課金することを特徴とする。

【００１０】さらに本発明は、前記情報端末装置が前記第一の通信手段を介して受信した暗号化情報が、前記第二の通信手段を介して受信した鍵情報を用いて正常に解読されなかった場合に、前記携帯端末装置は前記鍵情報の再送要求を前記第二の通信手段を介し送信することを特徴とする。

【００１１】さらに本発明は、前記情報端末装置が前記

第一の通信手段を介して受信した暗号化情報が、前記第二の通信手段を介して受信した鍵情報を用いて正常に解読された場合に、前記携帯端末装置は解読完了通知を前記第二の通信手段を介し送信することを特徴とする。

【００１２】本発明の携帯端末装置は、前記鍵情報を管理する鍵管理サーバが前記携帯端末への鍵情報送信の後、所定時間以内に携帯端末装置から解読完了通知を受信しない場合に、前記鍵管理サーバは鍵情報を第二の通信手段を介して再送することを特徴とする。

【００１３】さらに本発明は、第一の通信方式の信号を送受信する第一の通信手段と、前記第一の通信方式とは異なる第二の通信方式の信号を送受信する第二の通信手段とを具備し、暗号化された暗号化情報を前記第一の通信手段を介して送信及び又は受信し、前記暗号化情報を解読するための鍵情報を前記第二の通信手段を介して送信及び又は受信することを特徴とする。

【００１４】さらに本発明の携帯端末装置は、前記第一の通信方式は前記第二の通信方式よりも高速な通信方式であることを特徴とする。さらに本発明の携帯端末装置は、前記第一の通信手段を介して受信した暗号化情報が、前記第二の通信手段を介して受信した鍵情報を用いて正常に解読されなかった場合に、前記鍵情報の再送要求を前記第二の通信手段を介して行う再送要求手段を更に具備することを特徴とする。

【００１５】さらに本発明の携帯端末装置は、前記第一の通信手段を介して受信した暗号化情報が、前記第二の通信手段を介して受信した鍵情報を用いて正常に解読された場合に、解読完了通知を前記第二の通信手段を介して行う解読完了通知手段を更に具備することを特徴とする。

【００１６】

【発明の実施の形態】以下、図面を参照して本発明の実施の形態を説明する。図１は本発明の実施の形態に係わる情報提供システムの構成を示す構成図である。本実施の形態に係わる情報提供システムは、鍵管理サーバ１０１と、情報サーバ１０２と、通信網１０５と、第一の無線基地局１０３と、第二の無線基地局１０４と、少なくとも１台以上の携帯端末１０６とを含んで構成される。携帯端末１０６は第一の無線機地局１０３及び第二の無線基地局１０４と通信可能であり、第一の無線機地局１０３は第二の無線基地局１０４よりも高速な情報伝送が可能である。一方、第二の無線基地局１０４は第一の無線基地局１０３よりも地理的に広い範囲に通信サービスを提供する。情報サーバ１０２は携帯端末１０６に提供する情報を暗号化して蓄積し、鍵管理サーバ１０１はその暗号化してある情報を復号化するための鍵を蓄積する。鍵管理サーバ１０１と情報サーバ１０２と第一の無線基地局１０３と第二の無線基地局１０４は通信網１０５を介して接続されている。

【００１７】次に、以上のように構成された情報提供シ

5

ステムにおける情報配信方法の動作例を示す。図２及び図３は本発明の実施の形態の一例に係わる情報配信方法を示す流れ図である。利用者が情報を要求する場合は、利用者の所持する携帯端末１０６が情報要求を第二の無線基地局１０４に送信し、さらに第二の基地局は情報サーバ１０２に情報要求を送信する。ここで、携帯端末１０６は図４に示すように情報要求を第一の無線基地局１０３に送信しても良い。情報サーバ１０２は要求された情報を暗号化した形式で第一の無線基地局１０３を介して携帯端末１０６に送信する。暗号化された暗号化情報を受信した携帯端末１０６は、該暗号化情報を復号化するための鍵を必要とするため、鍵要求を第二の無線基地局１０４に送信する。該鍵要求を受信した第二の無線基地局１０４は鍵要求をさらに鍵管理サーバ１０１に送信する。該鍵管理サーバ１０１は要求された鍵を第二の無線基地局１０４を介して携帯端末１０６に送信する。ここで、図４あるいは図５の流れ図に示す情報配信方法の例のように、該鍵管理サーバ１０１は第二の無線基地局１０４を介して、該携帯端末１０６が正当な端末であるか否か認証を行なっても良い。該鍵管理サーバ１０１は該携帯端末１０６を正当な端末であると判断した場合に、要求された鍵を第二の無線基地局１０４を介して携帯端末１０６に送信する。該携帯端末１０６は該鍵を受信すると、暗号化された受信情報を復号することが可能である。鍵管理サーバ１０１では、該携帯端末に鍵を送信した後に課金をすることも可能である。

【００１８】また図６の流れ図に示すように、携帯端末１０６が鍵を受信して復号を行ない、正常に復号が完了すると、復号完了通知を第二の無線基地局１０４を介して鍵管理サーバ１０１に送信し、鍵管理サーバ１０１は該復号完了通知を受信した後課金を行なうことも可能である。

【００１９】一方、携帯端末１０６が予め契約をする情報提供システムの場合は、鍵管理サーバが鍵要求を受信した段階で携帯端末１０６が契約しているか否かを判断し、契約をしている場合にのみ鍵を携帯端末１０６に送信することも可能である。なお、以上では携帯端末１０６が情報を受信した後鍵を受信する例に関して述べたが、携帯端末１０６において鍵の受信の後に情報を受信しても良い。また、携帯端末１０６が複数の暗号化情報を要求して受信しておき、その後利用者が情報を見たくなった時に、見たい情報のみを復号化する鍵を要求して受信し、見たい暗号化情報だけを復号化してもよい。

【００２０】以上説明したように、携帯端末が高速な通信が可能な無線基地局から暗号化された情報を受信し、地理的に広い範囲で通信サービスの提供が可能な無線機地局から情報を復号化するための鍵を受信することにより、情報の短時間での受信及び地理的に広い範囲での暗号化情報の復号を可能にし、情報を正当な利用者にのみ伝達することが可能となる。また、地理的に広い範囲で

6

通信サービスを提供する通信システムでのみ、鍵や課金の管理を行なえば良い。特に、前記第二の無線基地局１０４として既存のPHS(Personal Handy phone System)基地局や自動車・携帯電話基地局を利用した場合、既存の加入者情報を利用し、新たに高速な通信が可能な第一の無線基地局を付加した場合、課金を既存の通信システムを利用して行なうことができ、低コストで高速な情報提供システムを構築することが可能となる。

【００２１】次に鍵の要求を携帯端末から出さない情報配信方法の動作例を示す。図７及び図８は本発明の他の実施の形態に係わる情報配信方法を示す流れ図である。

なお、本実施の形態に係わる情報提供システムの構成は図１に示す構成図と同様である。

【００２２】利用者が情報を要求する場合は、利用者の所持する携帯端末１０６が情報要求を第二の無線基地局１０４に送信し、さらに第二の基地局は情報サーバ１０２に情報要求を送信する。ここで、図７に示すように携帯端末１０６は第一の無線基地局１０３に情報要求を送信しても良い。情報サーバ１０２は要求された情報を暗号化した形式で第一の無線基地局１０３を介して携帯端末１０６に送信するが、これとは別に鍵要求を鍵管理サーバに送信し、該暗号化された情報を復号化するための鍵を該携帯端末１０６に送信するよう要求する。これは、携帯端末１０６が情報要求を出す際に、第二の無線基地局１０４を介して通信するための識別子を通知することにより可能である。鍵管理サーバ１０１は該鍵要求を受信すると、要求された鍵を第二の無線基地局１０４を介して携帯端末１０６に送信する。

【００２３】ここで、図９あるいは図１０の流れ図に示す情報配信方法の例のように、該鍵管理サーバ１０１は第二の無線基地局１０４を介して、該携帯端末１０６が正当な端末であるか否か認証を行なっても良い。該鍵管理サーバ１０１は該携帯端末１０６を正当な端末であると判断した場合に、要求された鍵を第二の無線基地局１０４を介して携帯端末１０６に送信する。携帯端末１０６は該鍵を受信すると、暗号化された受信情報を復号することが可能である。ここで、鍵管理サーバ１０１は携帯端末１０６に鍵を送信した後に課金をすることも可能である。また図６の流れ図に示すように、携帯端末１０６が鍵を受信して復号を行ない、正常に復号が完了すると、復号完了通知を第二の無線基地局１０４を介して鍵管理サーバ１０１に送信し、鍵管理サーバ１０１は該復号完了通知を受信した後課金を行なうことも可能である。一方、携帯端末１０６が予め契約をする情報提供システムの場合は、鍵管理サーバが鍵要求を受信した段階で携帯端末１０６が契約しているか否かを判断し、契約をしている場合にのみ鍵を携帯端末１０６に送信することも可能である。

【００２４】以上説明したように、携帯端末が高速な通信が可能な無線基地局から暗号化された情報を受信し、

地理的に広い範囲で通信サービスの提供が可能な無線基地局から情報を復号化するための鍵を受信することにより、情報の短時間での受信及び地理的に広い範囲での暗号化情報の復号を可能にし、情報を正当な利用者にのみ伝達することが可能となる。また、地理的に広い範囲で通信サービスを提供する通信システムでのみ、鍵や課金の管理を行なえば良い。特に、前記第二の無線基地局１０４としてPHS(Personal Handy phone System)基地局や自動車・携帯電話基地局を利用した場合、既存の加入者情報を利用し、新たに高速な通信が可能な第一の無線基地局を付加した場合、課金を既存の通信システムを利用して行なうことができ、低コストで高速な情報提供システムを構築することが可能となる。さらに、携帯端末から発呼して鍵を要求する必要がなく、利用者がより利用しやすい情報提供システムの構築が可能となる。

【００２５】次に暗号化情報及び鍵を受信した携帯端末が情報の復号ができない場合の情報配信方法の動作例を示す。図１１は本発明のその他の実施の形態に係わる情報配信方法を示す流れ図である。なお、本実施の形態に係わる情報提供システムの構成は図１に示す構成図と同様である。

【００２６】鍵管理サーバ１０１は鍵を第二の無線基地局１０４を介して携帯端末１０６に送信すると該携帯端末１０６あるいは該携帯端末１０６の利用者に対して課金を行なう。該鍵を受信した携帯端末１０６は該鍵を用いて情報の復号を行なう。ここで正常に情報が復号できない場合は、携帯端末１０６は復号不可通知を第二の基地局１０４を介して鍵管理サーバ１０１に送信し、正常に情報が復号できない旨送信する。鍵管理サーバ１０１は、前記鍵の送信の後に課金を行なっている場合は、該課金を取り消す。

【００２７】以上説明したように、携帯端末が受信した鍵で情報を復号できない場合には、復号付加通知を第二の無線基地局経由で送信することにより、既に課金されていても課金を取り消すことが可能である。また、第二の無線基地局は第一の無線基地局よりも地理的広い範囲をカバーしているので、復号が不可能な場合にその旨通知できる確率が高く、不正な課金を防止することが可能になる。

【００２８】次に暗号化情報及び鍵を受信した携帯端末が情報の復号ができない場合の情報配信方法の別の動作例を示す。図１２は本発明のその他の実施の形態に係わる情報配信方法を示す流れ図である。なお、本実施の形態に係わる情報提供システムの構成は図１に示す構成図と同様である。

【００２９】鍵管理サーバ１０１は鍵を第二の無線基地局１０４を介して携帯端末１０６に送信する。ここで、鍵管理サーバ１０１は該携帯端末１０６あるいは該携帯端末１０６の利用者に対して課金を行なってもよい。該鍵を受信した携帯端末１０６は該鍵を用いて情報の復号を行なう。ここで正常に情報が復号できない場合は、携帯端末１０６は鍵再送要求を第二の無線基地局１０４を介して鍵管理サーバ１０１に送信し、暗号化された情報を復号化する鍵を要求する。鍵管理サーバ１０１は要求に基づき、鍵を第二の無線基地局１０４を介して携帯端末１０６に送信する。ここで、図１３の流れ図に示す情報配信方法の例のように、該鍵管理サーバ１０１は第二の無線基地局１０４を介して、該携帯端末１０６が正当な端末であるか否か認証を行なっても良い。該鍵管理サーバ１０１は該携帯端末１０６を正当な端末であると判断した場合に、要求された鍵を第二の無線基地局１０４を介して携帯端末１０６に再送する。再送された鍵を受信した携帯端末１０６は該鍵を用いて情報の復号を行なう。ここで再度復号不可能な場合は、携帯端末１０６は再度鍵再送要求を鍵管理サーバに送信しても良い。

【００３０】また、復号不可通知を鍵管理サーバ１０１に送信して、既に課金されている場合は課金の取り消しを要求しても良い。以上説明したように、携帯端末が受信した鍵で情報を復号できない場合には、鍵再送要求を第二の無線基地局経由で送信することにより、鍵を再度得ることが可能となる。また、第二の無線基地局は第一の無線基地局よりも地理的広い範囲をカバーしているので、復号が不可能な場合に鍵を再度受信できる確率が高く、携帯端末で情報を正しく復号できる可能性を高めることが可能となる。

【００３１】次に暗号化情報及び鍵を受信した携帯端末が情報の復号ができない場合の情報配信方法の別の動作例を示す。図１４は本発明のその他の実施の形態に係わる情報配信方法を示す流れ図である。なお、本実施の形態に係わる情報提供システムの構成は図１に示す構成図と同様である。

【００３２】鍵管理サーバ１０１は鍵を第二の無線基地局１０４を介して携帯端末１０６に送信する。該鍵を受信した携帯端末１０６は該鍵を用いて情報の復号を行なう。ここで図６の流れ図に示すように、携帯端末１０６において正常に情報が復号できた場合は、携帯端末１０６は復号完了通知をを第二の無線基地局１０４を介して鍵管理サーバ１０１に送信し、鍵管理サーバ１０１は所定時間以内に該復号完了通知を受信すると課金を行なってもよい。しかし、携帯端末１０６において正常に情報が復号できない場合には復号完了通知を送信しない。そのため、鍵管理サーバ１０１は鍵送信の後所定時間経過するとタイムアウトとなり、鍵を再送する。ここで、図１５の流れ図に示す情報配信方法の例のように、この鍵の再送の前に該鍵管理サーバ１０１は第二の無線基地局１０４を介して、該携帯端末１０６が正当な端末であるか否か認証を行なっても良い。該鍵管理サーバ１０１は該携帯端末１０６を正当な端末であると判断した場合に、要求された鍵を第二の無線基地局１０４を介して携帯端末１０６に再送する。携帯端末１０６は該鍵を再び

9

受信し情報を復号することが可能となる。ここで、携帯端末１０６において情報が正常に復号できれば、図６の流れ図に示すように携帯端末１０６は復号完了通知を鍵管理サーバ１０１に送信すれば良い。一方正常に復号できない場合には、携帯端末１０６は復号完了通知を送信しないので、鍵管理サーバから鍵を再び受信することができる。

【００３３】以上説明したように、携帯端末が受信した鍵で情報を復号できない場合には、鍵を再度得ることが可能となる。また、第二の無線基地局は第一の無線基地局よりも地理的広い範囲をカバーしているので、復号が不可能な場合に鍵を再度受信できる確率が高く、携帯端末で情報を正しく復号できる可能性を高めることが可能となる。

【００３４】

【発明の効果】以上説明したように本発明の情報配信方法では、利用者が要求した大容量の情報を、非常に短時間で携帯端末に送信することを可能にしつつ、より正確な課金を行なうことを可能にする。また、既存の低速な通信システムを活用しつつ、低コストで課金管理を行なうことが可能である。

【００３５】さらに、認証を携帯端末への情報の送信とは別に行なうことを可能にするため、携帯端末への情報の送信に要する時間を短縮し、情報を送信するチャネルの利用効率を向上させることが可能となる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係わる情報提供システムの構成を示す説明図である。

【図２】本発明の実施例に係わる情報配信方法を示す流れ図で、特に携帯端末が第二の無線基地局を介して情報要求を行なう場合の流れ図である。

【図３】本発明の実施例に係わる情報配信方法を示す流れ図で、特に携帯端末が第一の無線基地局を介して情報要求を行なう場合の流れ図である。

【図４】本発明の実施例に係わる情報配信方法を示す流れ図で、特に鍵管理サーバが携帯端末の認証を行なう場合の流れ図である。

【図５】本発明の実施例に係わる情報配信方法を示す流れ図で、特に鍵管理サーバが携帯端末の認証を行なう場合の流れ図である。

10

【図６】本発明の実施例に係わる情報配信方法を示す流れ図で、特に携帯端末が復号完了通知を送信する場合の流れ図である。

【図７】本発明の実施例に係わる情報配信方法を示す流れ図で、特に携帯端末が第二の無線基地局を介して情報要求を行なう場合の流れ図である。

【図８】本発明の実施例に係わる情報配信方法を示す流れ図で、特に携帯端末が第一の無線基地局を介して情報要求を行なう場合の流れ図である。

【図９】本発明の実施例に係わる情報配信方法を示す流れ図で、特に鍵管理サーバが携帯端末の認証を行なう場合の流れ図である。

【図１０】本発明の実施例に係わる情報配信方法を示す流れ図で、特に鍵管理サーバが携帯端末の認証を行なう場合の流れ図である。

【図１１】本発明の実施例に係わる情報配信方法を示す流れ図で、特に携帯端末が復号不可通知を送信する場合の流れ図である。

【図１２】本発明の実施例に係わる情報配信方法を示す流れ図で、特に携帯端末が鍵の再送要求を行なう場合の流れ図である。

【図１３】本発明の実施例に係わる情報配信方法を示す流れ図で、特に鍵管理サーバが鍵の再送時に携帯端末の認証を行なう場合の流れ図である。

【図１４】本発明の実施例に係わる情報配信方法を示す流れ図で、特に鍵管理サーバがタイムアウトにより鍵を再送する場合の流れ図である。

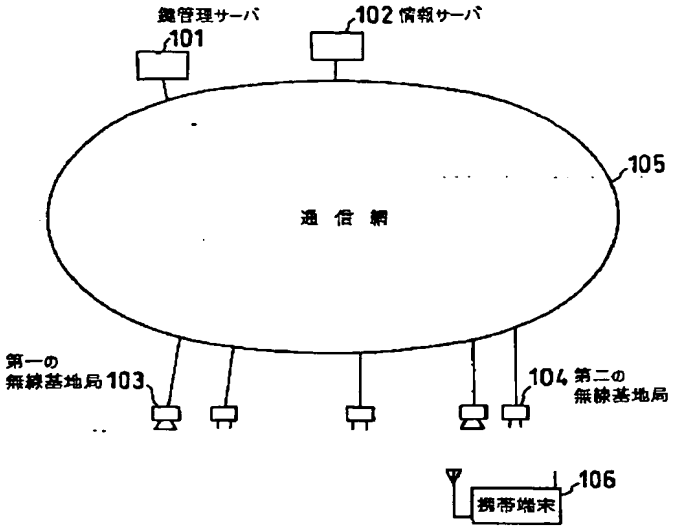
【図１５】本発明の実施例に係わる情報配信方法を示す流れ図で、特に鍵管理サーバが鍵の再送時に携帯端末の認証を行なう場合の流れ図である。

【図１６】従来の情報配信方法に係わる情報提供システムの構成を示す構成図である。

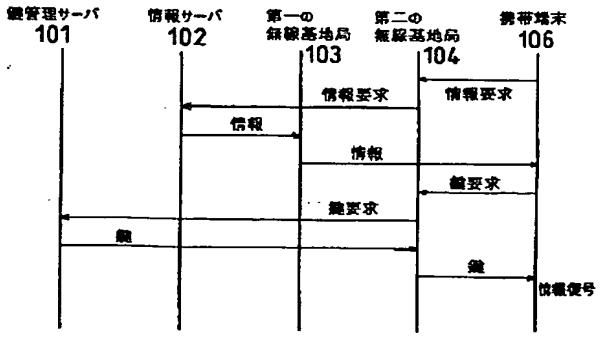
【符号の説明】

１０１…鍵管理サーバ
１０２…情報サーバ
１０３…第一の無線基地局
１０４…第二の無線基地局
１０５…通信網
１０６…携帯端末

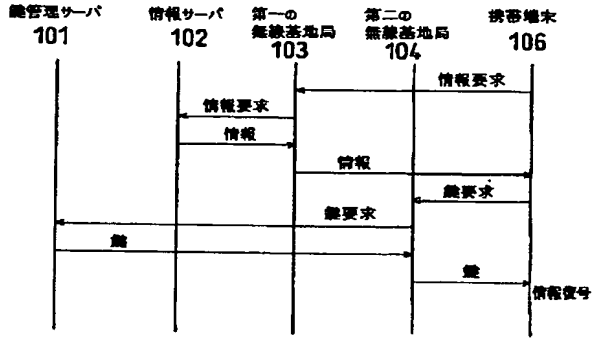
【図１】



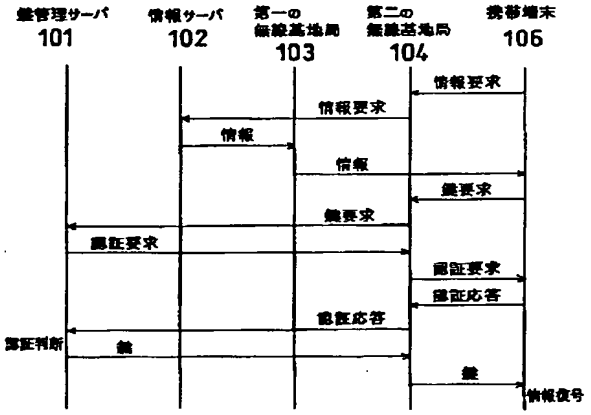
【図２】



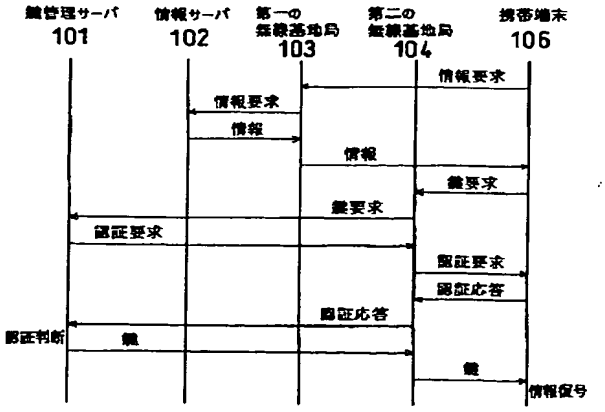
【図３】



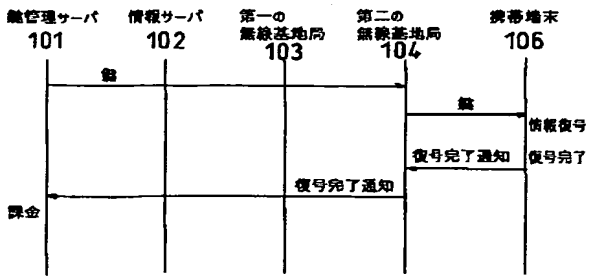
【図４】



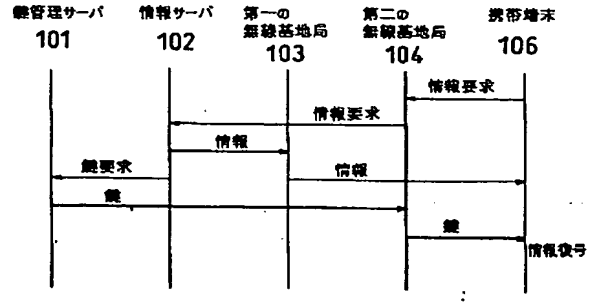
【図５】



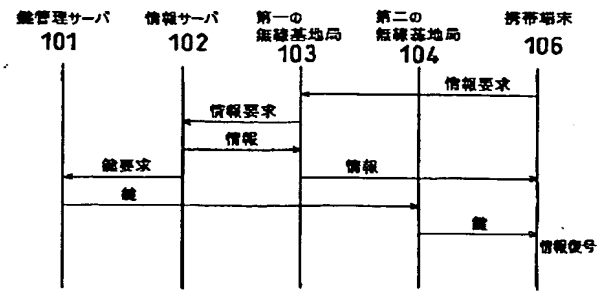
【図６】



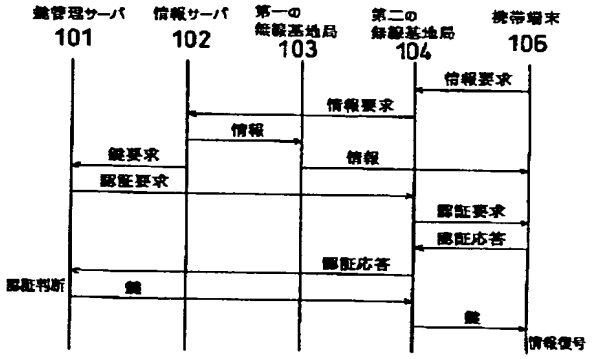
【図７】



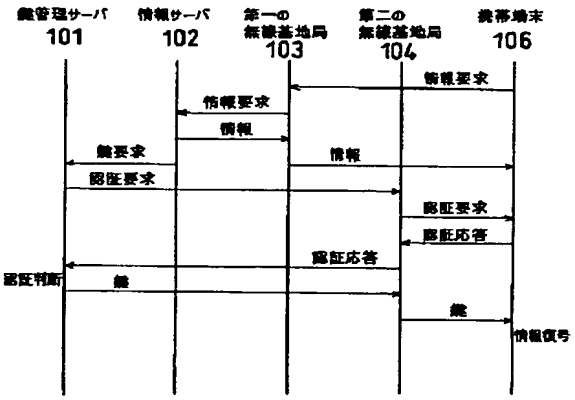
【図８】



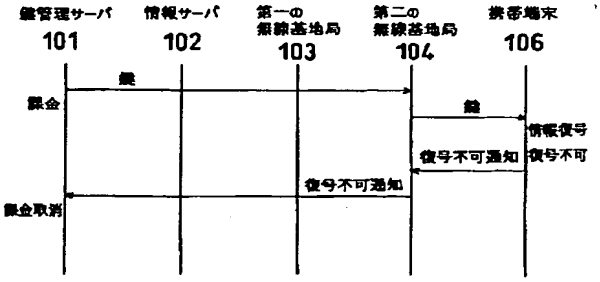
【図９】



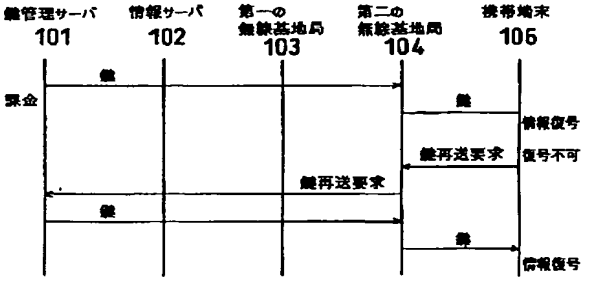
【図１０】



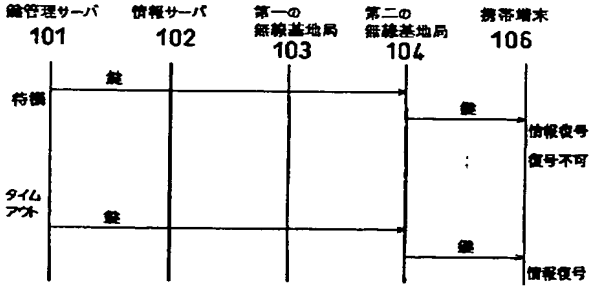
【図１１】



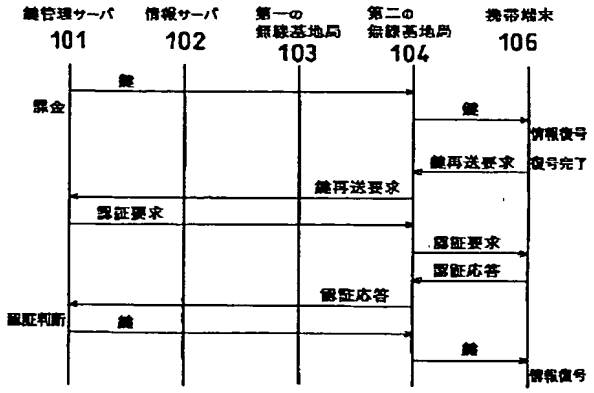
【図１２】



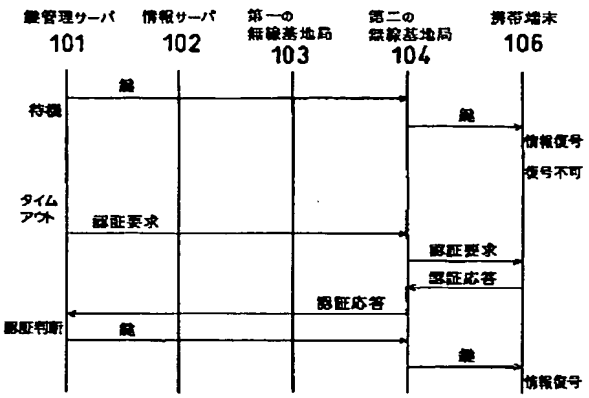
【図１４】



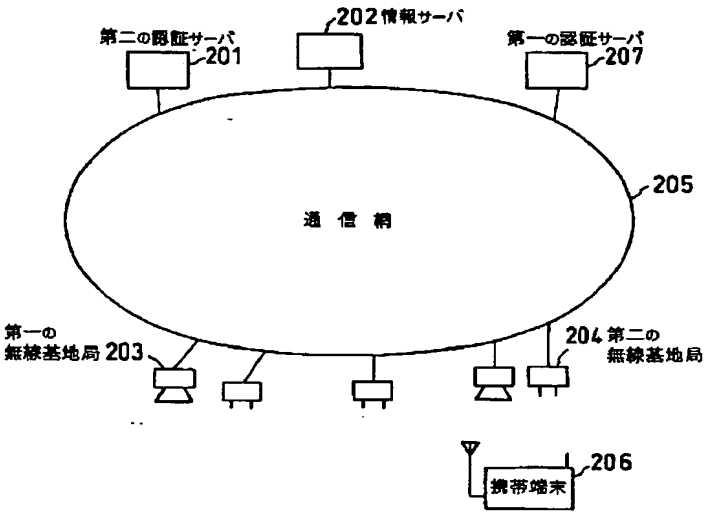
【図１３】


鍵管理サーバ
101
情報サーバ
102
第一の
無線基地局
103
第二の
無線基地局
104
携帯端末
106
鍵
課金
鍵
情報復号
鍵再送要求
復号完了
鍵再送要求
認証要求
認証要求
認証応答
認証応答
認証判断
鍵
鍵
情報復号

【図１５】


鍵管理サーバ
101
情報サーバ
102
第一の
無線基地局
103
第二の
無線基地局
104
携帯端末
106
鍵
待機
鍵
情報復号
復号不可
タイム
アウト
認証要求
認証要求
認証応答
認証応答
認証判断
鍵
鍵
情報復号

【図１６】


第二の認証サーバ
201
202情報サーバ
第一の認証サーバ
207
205
通信網
第一の
無線基地局 203
204 第二の
無線基地局
206
携帯端末

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/08230

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] H04H 1/00
H04Q 7/38
H04M 11/08
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] H04H 1/00- 1/02 H04B 7/24- 7/26
H04Q 7/00- 7/38 H04M 11/00-11/10
H04M 3/42- 3/58 G10K 15/00-15/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Toroku Jitsuyo Shinan Koho 1994-2001
Kokai Jitsuyo Shinan Koho 1971-2001 Jitsuyo Shinan Toroku Koho 1996-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	JP, 09-282278, A (Ricoh Company, Ltd.), 31 October, 1997 (31.10.97), column 12, lines 5-46 (Family: none)	1,2,9,11,14,15 4,5-8,10,12, 13,16,17 3
Y	JP, 10-200493, A (Toshiba Corporation), 31 July, 1998 (31.07.98), Full text (Family: none)	4-9,12,13,16, 17
Y	JP, 10-136123, A (Hitachi Zosen Corporation), 22 May, 1998 (22.05.98), Column 4, lines 5-42 (Family: none)	5,6,10,13,17
Y	JP, 11-266483, A (Toshiba Corporation), 28 September, 1999 (28.09.99), Column 2, lines 35 to column 3, line 27 (Family: none)	5,6,13,17
Y	EP, 0831608, A2 (AT & T Corp.), 11 August, 1997 (11.08.97), (ALL DOCUMENT) & JP, 10-190594, A	7,8

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 February, 2001 (20.02.01)	06 March, 2001 (06.03.01)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP00/08230

(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 11-164058, A (Hitachi Electron Service Co., Ltd.), 13 June, 1999 (13.06.99), Full text (Family: none)	4
A	JP, 08-221087, A (BROTHER INDUSTRIES, LTD.), 30 August, 1996 (30.08.96), Column 7, line 30 to Column 8, line 1 (Family: none)	3